

Portable electronic door opener device and method for secure door opening

ABSTRACT OF THE INVENTION

A portable computing device for opening a door (an electronic door opener) and a method for its use is disclosed. The computing device has a shared secret key, a standard certificate, means for communicating with the door, and a processor adapted for performing operations with shared secret keys and standard certificates. The door also possesses the same shared secret key. Under normal operation, messages encoded with the shared secret key serve to establish a right to open the door. The portable computing device's standard certificate is used to respond to occasional challenges by the door, and to generate the shared secret key. Biometric capabilities of the portable computing device add an additional layer of security in screening the identity of the user of the device. A security system for controlling access, involving a first plurality of computing devices and a second plurality of doors, and operating based on shared secret keys and occasional challenges is also disclosed.